Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Eternity Threat group is actively evolving its malware arsenal

Date of Publication

October 7, 2022

Admiralty Code

A1

TA Number

TA2022215

Summary

The Eternity group (also known as Eternity Team or Eternity Project), a Russian "Jester Group"-affiliated threat group, has been active since at least January 2022. Eternity uses a malware-as-a-service subscription model to disseminate multiple malware modules, including a new piece of malware named LilithBot, on underground forums.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	**T1003** OS Credential Dumping	**T1552** Unsecured Credentials	**T1552.002** Credentials in Registry
T1114 Email Collection	**T1114.002** Remote Email Collection	**T1005** Data from Local System	**TA0002** Execution
T1204 User Execution	**TA0005** Defense Evasion	**T1222** File and Directory Permissions Modification	**T1027** Obfuscated Files or Information
TA0007 Discovery	**T1016** System Network Configuration Discovery	**T1012** Query Registry	**T1018** Remote System Discovery
T1057 Process Discovery	**TA0002** Execution	**T1047** Windows Management Instrumentation	**T1059** Command and Scripting Interpreter
TA0003 Persistence	**T1037** Boot or Logon Initialization Scripts	**T1037.005** Startup Items	**TA0011** Command and Control
T1071 Application Layer Protocol			

Technical Details

#1 Latest LilithBot malware variant inspects for the presence of several DLLs and Win32 PortConnector to validate that the LilithBot is running on a host machine rather than a virtual machine.

#2 Following a successful intrusion, the botnet harvests files and user information such as browser history, cookies, images, and screenshots, which are bundled into a ZIP archive "report.zip" and exfiltrated via a command-and-control (C2) server.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-1	0ebe8de305581c9eca37e53a46d033c8 1cae8559447370016ff20da8f717db53 e793fcd5e44422313ec70599078adbdc 65c0241109562662f4398cff77499b25
IPV4	77[.]73.133.12 45[.]9.148.203 91[.]243.59.210 195[.]2.71.214

References

https://www.zscaler.com/blogs/security-research/analysis-lilithbot-malware-and-eternity-threat-group

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

October 7, 2022 • 9:34 AM

More at www.hivepro.com